Quantum theory from rules on information acquisition

Philipp Andres Höhn

Vienna Center for Quantum Science and Technology, and Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences, Boltzmanngasse 3, 1090 Vienna, Austria

E-mail: p.hoehn@univie.ac.at

Abstract. We provide an accessible and mostly self-contained summary of a recent reconstruction of quantum theory, for qubit systems, from rules constraining an observer's acquisition of information. The focus lies on the main ideas and results, not the technical details. This reconstruction offers an instructive, informational explanation for the architecture of the theory and, as a by-product, unravels new 'conserved informational charges', indeed appearing in quantum theory, that characterize the unitary group and the set of pure states.

1. Introduction

What makes quantum theory special? In order to even sensibly ask this question, we have to step beyond quantum theory and consider it within a landscape of alternative theories, permitting us to ponder about how the world *could* have been different. It requires us to leave the usual textbook formulation of quantum theory and everything we take for granted about it behind and to develop a more general language that also applies to alternative theories. Ideally, this language should be operational, encompassing the interactions of some observer with physical systems in a plethora of conceivable, physically distinct worlds.

In order to also answer the above question, we then have to find *physical* properties of quantum theory that single it out, at least within the given landscape of alternatives. In particular, the goal should be to find an operational justification for the textbook axioms, i.e., for complex Hilbert spaces, unitary dynamics, state linearity, tensor product structure for composite systems, Born rule, and so on. The result is a reconstruction of quantum theory from operational axioms [1–10] – and ideally a better understanding of what quantum theory tells us about Nature.

In this manuscript, we shall review and summarize how the quantum formalism for arbitrarily many qubits can be reconstructed from operational rules restricting an observer's acquisition of information about the observed systems [1, 2]. The goal of this summary is to provide a didactical and easily accessible overview over this reconstruction. Its underlying framework is especially engineered for unraveling the architecture of quantum theory. In fact, as we shall see, the reconstruction will provide a transparent, informational explanation for the structure of qubit quantum theory and thereby also for its paradigmatic features such as entanglement and monogamy. The approach also produces novel 'conserved informational charges', indeed appearing in quantum theory, that turn out to characterize the unitary group and the set of pure states and which might find practical applications in quantum information.

The premise of the summarized approach is to only speak about information that the observer has access to. It is thus purely operational and survives without any ontological commitments. This approach is inspired, in part, by Rovelli's *relational quantum mechanics* [11] and the Brukner-Zeilinger informational interpretation of quantum theory [12,13]; the successful reconstruction can be viewed as a completion of these ideas.

The rest of the manuscript is organized as follows. In sec. 2, we review the landscape of alternative theories, in sec. 3, we formulate the operational quantum axioms, in sec. 4, we summarize the key steps of the reconstruction itself and, finally, conclude in section 5.

2. Overview over a landscape of theories

We shall begin with an overview over a landscape of alternative theories which has been developed in [1, 2] to which we also refer for further details.

2.1. From questions and answers to probabilities and states

Consider an observer O who interrogates an ensemble of (identical) systems $\{S_a\}_{a=1}^n$, coming out of a preparation device, with binary questions Q_i from some set $\mathcal{Q}$. For example, in the case of quantum theory, such a question could read "is the spin of the electron up in x-direction?." This set $\mathcal{Q}$ shall only contain *repeatable* questions, the answers to which are not independent of S_a's preparation. We shall assume any S_a to always give a definite answer if asked some $Q_i \in \mathcal{Q}$; accordingly, $\mathcal{Q}$ can only contain physically implementable questions which are 'answerable' by the $\{S_a\}$ and not arbitrary logically conceivable binary questions. Also, since we assume definite answers we do not address the measurement problem. The answers to the $Q_i \in \mathcal{Q}$ given by the $\{S_a\}$ shall follow a specific statistics for each way of preparing the $\{S_a\}$ (for n sufficiently large). The set of all the possible answer statistics for all $Q_i \in \mathcal{Q}$ for all preparations is denoted by Σ.

O, being a good experimenter, has developed, through his experiments, a theoretical model for $\mathcal{Q}$ and Σ which he employs to interpret the outcomes of his interrogations (and to decide whether a question is in $\mathcal{Q}$ or not). This permits O to assign, for the next S_a to be interrogated, a prior probability y_i that S_a's answer to $Q_i \in \mathcal{Q}$ will be 'yes'. Namely, O determines y_i through a Bayesian updating according to his model of Σ, any prior information on the way of preparation, and to the frequencies of 'yes' answers to questions from $\mathcal{Q}$ which he recorded in previous interrogation runs on systems identically prepared to S_a (more on this below).

While $\mathcal{Q}$ need not necessarily contain *all* binary measurements that O could, in principle, perform on the $\{S_a\}$, we shall assume that $\mathcal{Q}$ is 'tomographically complete' in the sense that the $\{y_i\}_{\forall Q_i \in \mathcal{Q}}$ are sufficient to compute the probabilities for all other physically realizable measurements possibly not contained in the $\mathcal{Q}$ too. Hence, the y_i encode everything O could possibly say about the outcomes to arbitrary experiments on the $\{S_a\}$ in his laboratory. It will therefore be sufficient to henceforth restrict O to acquire information about the S_a solely through the $Q_i \in \mathcal{Q}$. It is also natural to identify O's 'catalogue of knowledge' about the given S_a, i.e. the collection of $\{y_i\}_{\forall Q_i \in \mathcal{Q}}$, with *the state of S_a relative to O*. This is a state of information and an element of Σ. Conversely, any element in Σ assigns a probability y_i to all $Q_i \in \mathcal{Q}$. Thus, we identify Σ with the *state space* of S_a.

2.2. Time evolution of O's 'catalogue of knowledge'

We permit O to subject the $\{S_a\}$ to interactions which cause a state $\{y_i(t_0)\}_{\forall Q_i \in \mathcal{Q}}$ at time t_0 to evolve in time to another legitimate state. Any permitted time evolution shall be temporally translation invariant, thus defining a one-parameter map $T_{\Delta t}(\{y_i(t_0)\}_{\forall Q_i \in \mathcal{Q}}) = \{y_i(t_0 + \Delta t)\}_{\forall Q_i \in \mathcal{Q}}$ from Σ to itself which only depends on the time interval Δt but not on t_0. We denote by $\mathcal{T}$ the set of all time evolutions to which we allow O to expose the $\{S_a\}$.

Clearly, $\mathcal{T}$ is a further crucial ingredient of O's world model; his model for describing his interrogations with the $\{S_a\}$ is thus encoded in the triple $(\mathcal{Q}, \Sigma, \mathcal{T})$.

2.3. Convexity and state of no information

It will be our challenge to unravel what O's world model is. This requires us to subject the triple $(\mathcal{Q}, \Sigma, \mathcal{T})$ to a number of further operational conditions that are 'natural' in the context of information acquisition with a Bayesian spirit. Upon imposing the quantum postulates, this will turn out to restrict $\mathcal{Q}$ and $\mathcal{T}$ to incorporate only a 'natural' subset of all possible quantum measurements and time evolutions, namely projective binary measurements and unitaries, respectively (rather than arbitrary positive operator-valued measures (POVMs) and completely positive maps). But this suffices for our purposes to reconstruct the textbook quantum formalism.

First, to account for the possibility of randomness in the method of preparation, we assume Σ to be convex. Consider a collection of identical systems (i.e., with identical $(\mathcal{Q},\Sigma,\mathcal{T})$) that are not necessarily in identical states and for which O uses a cascade of biased coin tosses to decide which system to interrogate. Then O is enabled to assign a single prior state to this collection which is a convex combination of their individual states.

Next, we assume the existence of a special method of preparation which generates even completely random answer statistics over all $Q_i \in \mathcal{Q}$. This preparation is described by a special state in Σ, namely $y_i = \frac{1}{2}$, $\forall\, Q_i \in \mathcal{Q}$, and shall be called the *state of no information.* This distinguished state is a constraint on the *pair* $(\mathcal{Q},\Sigma)$[1] and plays two crucial roles: it defines (1) the prior state of S_a that O will start with in a Bayesian updating when he has no 'prior information' about the $\{S_a\}$ (except what his model $(\mathcal{Q},\Sigma,\mathcal{T})$ is); and (2) an unambiguous notion of *(in-)dependence* of questions (cf. sec. 2.4) which otherwise would be state dependent.[2]

2.4. State updating and (in)dependence and compatibility of questions

There are two kinds of state update rules, one for the state of the ensemble $\{S_a\}$ (which coincides with the prior state assigned to the next S_a to be interrogated) and one for the posterior state of a given ensemble member S_a. In a *single shot interrogation*, O receives a single S_a, assigns a prior state to it according to his prior information (cf. sec. 2.1), interrogates it with some questions from $\mathcal{Q}$ (without intermediate re-preparation) and, depending on the answers, updates the prior to a posterior state valid for this specific S_a only. This requires a consistent *posterior state update rule* which permits O to update the probabilities y_i for all $Q_i \in \mathcal{Q}$ in a manner that respects the structure of Σ and the repeatability of questions (i.e., an answer Q_i = 'yes' or 'no' must have a posterior $y_i = 1$ or 0 as a consequence, respectively). This is *not* a Bayesian updating. Specifically, the posterior state of S_a may differ significantly from its prior state if O has experienced an information gain on at least some $Q_i \in \mathcal{Q}$. (This will necessarily happen when complementary questions are involved, see below.) This is the 'collapse' of the state: it is merely O's update of information about the specific S_a [1].

By contrast, in a *multiple shot interrogation*, O carries out a single shot interrogation on an entire (identically prepared [1]) ensemble $\{S_a\}$ to do *ensemble state tomography* and estimate the state of the ensemble from his prior information about the preparation and the collection of posterior states from the single shot interrogations. With every further interrogated S_a, O updates the ensemble state – which coincides with the prior state of the next system from the ensemble to be interrogated. Accordingly, this requires a *prior state update rule.* This *is* the Bayesian updating alluded to in secs. 2.1 and 2.3.

It will not be necessary to specify these two update rules in detail; we just assume O uses consistent ones. Specifically, given a posterior state update rule, we shall call $Q_i, Q_j \in \mathcal{Q}$

(maximally) independent if, after having asked Q_i to S in the state of no information, the posterior probability $y_j = \frac{1}{2}$. That is, if the answer to Q_i relative to the state of no information tells O 'nothing' about the answer to Q_j.

[1] E.g., in quantum theory ({binary POVMs}, {density matrices}) does not satisfy this condition because there exist inherently biased POVMs, while ({projective binary measurements}, {density matrices}) does.

[2] E.g., in quantum theory, the questions Q_{x_1} = "Is the spin of qubit 1 up in x-direction?" and Q_{x_2} = "Is the spin of qubit 2 up in x-direction?" are independent relative to the completely mixed state, however, not relative to a state with entanglement in x-direction.

(partially or maximally) dependent if, after having asked Q_i to S in the state of no information, the posterior probability $y_j \neq \frac{1}{2}$. That is, if the answer to Q_i relative to the state of no information gives O at least partial information about the answer to Q_j.

(maximally) compatible if O may know the answers to both Q_i, Q_j simultaneously, i.e. if there exists a state in Σ such that y_i, y_j can be simultaneously 0 or 1.

(maximally) complementary if every state in Σ which features $y_i = 0, 1$ necessarily implies $y_j = \frac{1}{2}$. Notice that complementarity implies independence (but not vice versa).

(One can also define partial compatibility similarly [1].) These relations shall be symmetric; e.g. Q_i is independent of Q_j if and only if Q_j is independent of Q_i, etc.

We impose a final condition on the posterior state update rule: if Q_i, Q_j are maximally compatible and independent then asking Q_i shall not change y_j, i.e. O's information about Q_j.

2.5. Informational completeness

The fundamental building blocks of the theories in the landscape which we are constructing are to be sets of pairwise independent questions. This will help to render the convoluted parametrization of a state by $\{y_i\}_{\forall Q_i \in \mathcal{Q}}$ more economical. Consider a set of pairwise independent questions $\mathcal{Q}_M := \{Q_1, \ldots, Q_D\}$; it is called *maximal* if no question from $\mathcal{Q} \setminus \mathcal{Q}_M$ can be added to $\mathcal{Q}_M$ without destroying pairwise independence of its elements. We shall assume that any maximal $\mathcal{Q}_M$ is *informationally complete* in the sense that *all* $\{y_i\}_{\forall Q_i \in \mathcal{Q}}$ can be computed from the corresponding probabilities $\{y_i\}_{i=1}^D$ for all states in Σ. Any such $\mathcal{Q}_M$ features D elements [1] such that Σ becomes a D-dimensional convex set and states become vectors

$$\vec{y} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_D \end{pmatrix}.$$

2.6. Information measure

Our focus is O's acquisition of information, so we need to quantify O's information about the systems. Since $Q_i \in \mathcal{Q}$ is binary, we quantify O's information about S_a's answer to it by a function $\alpha(y_i)$ with $0 \leq \alpha(y_i) \leq 1$ `bit` and $\alpha(y) = 0$ `bit` $\Leftrightarrow y = \frac{1}{2}$ and $\alpha(1) = \alpha(0) = 1$ `bit`. O's total information about a S_a must be a function of the state; we make an additive ansatz

$$I(\vec{y}) := \sum_{i=1}^{D} \alpha(y_i). \tag{1}$$

The quantum postulates will single out the specific function α.

Consider a set $\{Q_1, \ldots, Q_n\}$ of mutually (maximally) complementary questions. It is clear that whenever O has maximal information $\alpha(y_i) = 1$ `bit` about Q_i from this set, he must have 0 `bits` of information about all other questions in the set. We require more generally that such a set cannot support more than 1 `bit` of information, regardless of the state

$$\alpha(y_1) + \cdots + \alpha(y_n) \leq 1 \texttt{ bit} \tag{2}$$

for otherwise O could, for some states, *reduce* his total information about such a set by asking another question from it. These *complementarity inequalities* represent informational uncertainty relations that describe how the information gain about one question enforces an information loss about questions complementary to it (see also the state ‘collapse’ in sec. 2.4).

2.7. Composite systems and (classical) rules of inference

O must be able to tell a composite system apart into its constituents purely by means of the information accessible to him through interrogation and thus ultimately by means of the question sets. Let systems S_A, S_B have question sets $\mathcal{Q}_A, \mathcal{Q}_B$. It is then natural to say that they define a composite system S_{AB} if any $Q_a \in \mathcal{Q}_A$ is maximally compatible with any $Q_b \in \mathcal{Q}_B$ and if

$$\mathcal{Q}_{AB} = \mathcal{Q}_A \cup \mathcal{Q}_B \cup \tilde{\mathcal{Q}}_{AB}, \tag{3}$$

where $\tilde{\mathcal{Q}}_{AB}$ only contains composite questions which are iterative compositions, $Q_a *_1 Q_b, Q_a *_2 (Q_{a'} *_3 Q_b), (Q_a *_4 Q_b) *_5 Q_{b'}, (Q_a *_6 Q_b) *_7 (Q_{a'} *_8 Q_{b'}), \ldots$, via some logical connectives $*_1, *_2, *_3, \cdots$, of individual questions $Q_a, Q_{a'}, \ldots \in \mathcal{Q}_A$ about S_A and $Q_b, Q_{b'}, \ldots \in \mathcal{Q}_B$ about S_B. This definition is extended recursively to composite systems with more than two subsystems.

Since O can never test the truthfulness of statements about logical connectives of complementary questions through interrogations and since all propositions must have operational meaning, we shall permit O to logically connect two (possibly composite) questions *directly* with some $*$ only if they are compatible. For the same reason, O is allowed to apply classical rules of inference (in terms of Boolean logic) exclusively to sets of mutually compatible questions.

2.8. Computing probabilities and questions as vectors

Thanks to informational completeness, the probability function $Y(Q|\vec{y}) \in [0,1]$ that $Q =$'yes', given the state $\vec{y}$, exists for all $Q \in \mathcal{Q}$ and $\vec{y} \in \Sigma$. As shown in [2], the exhibited structure yields

$$Y(Q|\vec{y}) = Y(\vec{q}|\vec{y}) = \frac{1}{2}\left(\vec{q} \cdot (2\vec{y} - \vec{1}) + 1\right), \tag{4}$$

where $\vec{q} \in \mathbb{R}^D$ is a *question vector* encoding $Q \in \mathcal{Q}$ and $\vec{1}$ is a vector with each coefficient equal to 1 in the basis corresponding to $\mathcal{Q}_M$. This equation gives rise to (part of) the Born rule.

Suppose $Q, Q' \in \mathcal{Q}$ were both encoded by the same $\vec{q}$. Then, by (4), they would be probabilistically indistinguishable and O must view them as logically equivalent. O is free to remove any such redundancy from his description of $\mathcal{Q}$ upon which every permissible question vector $\vec{q}$ will encode a *unique* $Q \in \mathcal{Q}$. Finally, for every $Q \in \mathcal{Q}$ there exists a state $\vec{y}_Q$ which is the updated posterior state of S_a after O received a 'yes' answer to the single question Q from S_a in the (prior) state of no information. O had 0 `bits` of information before and $\vec{y}_Q$ encodes a single independent question answer, so we naturally require that it encodes 1 independent `bit`. Hence, for every $Q \in \mathcal{Q}$ there exists $\vec{y}_Q \in \Sigma$ with $I(\vec{y}_Q) = 1$ `bit` such that $Y(Q|\vec{y}_Q) = 1$.

3. The quantum principles as rules constraining O's information acquisition

In the sequel, we consider the most elementary of information carriers. Within the introduced landscape of theories, we now establish rules on O's acquisition of information that single out the quantum theory of a composite system S_N of $N \in \mathbb{N}$ qubits, modelled in our language by a triple $(\mathcal{Q}_N, \Sigma_N, \mathcal{T}_N)$. Effectively, these rules constitute a set of 'coordinates' for quantum theory on this landscape. The rules are spelled out first colloquially, then mathematically and are motivated in more detail in [1, 2].

Empirically, the information accessible to an experimenter about (characteristic properties of) elementary systems is limited. For example, an experimenter may know one binary proposition about an electron (e.g., its spin in x-direction), but nothing fully independent of it (and similarly for a classical bit). We shall characterize a composition of N elementary systems according to how much information is, in principle, simultaneously available to O.

Principle 1. (Limited Information) "The observer O can acquire maximally $N \in \mathbb{N}$ *independent* `bits` of information about the system S_N at any moment of time."
There exists a maximal set Q_i, $i = 1, \ldots, N$, of N mutually maximally independent and compatible questions in $\mathcal{Q}_N$.

O can thereby distinguish maximally 2^N states of S_N in a single shot interrogation.

But, empirically, elementary systems admit more independent propositions than what – due to the information limit – they are able to answer at a time. This is Bohr's complementarity. The unanswered properties must be random (and so 'in superposition') because the information limit makes it impossible to ascribe definite outcomes to them. For example, an experimenter may also inquire about the spin of the electron in y-direction. Yet doing so is at the total expense of his information about its spin in the x- and z-directions and subsequent such measurements have random outcomes. For the N elementary systems, we assert the existence of complementarity.

Principle 2. (Complementarity) "The observer O can always get up to N *new* independent `bits` of information about the system S_N. But whenever O asks S_N a new question, he experiences no net loss in his total amount of information about S_N."
There exists another maximal set Q'_i, $i = 1, \dots, N$, of N mutually maximally independent and compatible questions in $\mathcal{Q}_N$ such that Q'_i, Q_i are maximally complementary and $Q'_i, Q_{j \neq i}$ are maximally compatible.

The peculiar mathematical form of principle 2 becomes intuitive upon recalling that S_N is a *composite* system such that complementarity should exist *per* elementary system [1].

Principles 1 and 2 are conceptually inspired by (non-technical) proposals made by Rovelli [11] and Zeilinger and Brukner [12,13]. These principles say nothing about what happens in-between interrogations. Naturally, we demand O not to gain or lose information *without* asking questions.

Principle 3. (Information Preservation) "The total amount of information O has about (an otherwise non-interacting) S_N is preserved in-between interrogations."
$I(\vec{y})$ *is* constant *in time in-between interrogations for (an otherwise non-interacting) S_N.*

Hence, O's total information $I(\vec{y})$ is a 'conserved charge' of any time evolution $T_{\Delta t} \in \mathcal{T}_N$.

The more interactions to which O may subject S_N are available, the more ways in which any state may, in principle, change in time and thus the more 'interesting' O's world. We therefore demand that *any* time evolution is physically realizable as long as it is consistent with the other rules. (Since $\Sigma_N, \mathcal{T}_N$ are interdependent, this is distinct from 'maximizing the number' of states.)

Principle 4. (Time Evolution)[3] "O's 'catalogue of knowledge' about S_N evolves *continuously* in time in-between interrogations and every consistent such evolution is physically realizable."
$\mathcal{T}_N$ is the maximal set of transformations $T_{\Delta t}$ on states such that, for any fixed *state $\vec{y}$, $T_{\Delta t}(\vec{y})$ is* continuous *in Δt and compatible with principles 1-3 (and the structure of the theory landscape).*

We shall also allow O to ask *any* question to S_N which 'makes (probabilistic) sense'.

Principle 5. (Question Unrestrictedness)[4] "Every question which yields legitimate probabilities for every way of preparing S_N is physically realizable by O."
Every question vector $\vec{q} \in \mathbb{R}^{D_N}$ which satisfies $Y(\vec{q}|\vec{y}) \in [0,1]$ $\forall\, \vec{y} \in \Sigma_N$ and for which there exists $\vec{y}_Q \in \Sigma_N$ with $I(\vec{y}_Q) = 1$ `bit` such that $Y(\vec{q}|\vec{y}_Q) = 1$ corresponds to a $Q \in \mathcal{Q}_N$.

These five rules turn out to leave two solutions for the triple $(\mathcal{Q}_N, \Sigma_N, \mathcal{T}_N)$. Remarkably, they cannot distinguish between complex and real numbers. Namely, the two solutions are qubit and rebit quantum theory, i.e. two-level systems over real Hilbert spaces [1, 2]. Since the latter is both mathematically and physically a subcase of the former, these five rules can be regarded as sufficient. However, if one also wishes to discriminate rebits operationally, then an extra rule, adapted from [4, 5] and imposed *solely* for this purpose (it is partially redundant), succeeds.

[3] If we did not require this 'maximality' of $\mathcal{T}_N$, we would still ultimately obtain a linear, unitary evolution, but not necessarily the full unitary group. This is the sole reason for demanding 'maximality'. Note that principles 3 and 4 are *not* equivalent to the axiom of 'continuous reversibility' of generalized probabilistic theories [3–5].

[4] Without principle 5, we would still obtain the structure of an informationally complete set $\mathcal{Q}_{M_N}$, finding that it encodes a basis of projective Pauli operator measurements [2]; principle 5 legalizes all such measurements.

Principle 6. (Tomographic Locality) "O can determine the state of the composite system S_N by interrogating only its subsystems."

As shown in [1,2], principles 1–6 are equivalent to the textbook axioms. More precisely:

Claim. *The only solution to principles 1–6 is qubit quantum theory where*

- $\Sigma_N \simeq$ *convex hull of* $\mathbb{CP}^{2^N-1}$ *is the space of* $2^N \times 2^N$ *density matrices over* $\mathbb{C}^{2^N}$,
- *states evolve unitarily according to* $\mathcal{T}_N \simeq \mathrm{PSU(2^N)}$ *and the equation describing the state dynamics is (equivalent to) the von Neumann evolution equation,*
- $\mathcal{Q}_N \simeq \mathbb{CP}^{2^N-1}$ *is (isomorphic to) the set of projective measurements onto the* $+1$ *eigenspaces of* N*-qubit Pauli operators*[5] *and the probability for* $Q \in \mathcal{Q}_N$ *to be answered with 'yes' in some state is given by the Born rule for projective measurements.*

4. Synopsis of the reconstruction steps and key results

Since this gives rise to a *constructive* derivation of the explicit architecture of qubit quantum theory, it involves a large number of individual steps compared to the rather abstract reconstructions [3–5]. However, this is also rewarding as it offers novel informational explanations for typical features of quantum theory and so many reconstruction steps are actually quite instructive. We now provide a summary of key results and reconstruction steps from [1,2] (to which we refer for technical details) needed for proving the claim of the previous section.

4.1. Logical connectives for building informationally complete sets

The first task is to build informationally complete sets $\mathcal{Q}_{M_N}$ [1]. The conjunction of principles 1 and 2 implies that $\mathcal{Q}_{M_1} = \{Q_1, Q_2, \ldots, Q_{D_1}\}$ for a single elementary system must be a maximal mutually complementary set with $D_1 \geq 2$. We changed notation slightly, labelling complementary questions by numbers, not primes. Of course, in quantum theory, $D_1 = 3$; the more involved $N = 2$ case will entail this. The structure (3) of a composite system implies that $\mathcal{Q}_{M_2}$ should contain individual questions about its subsystems. Continuing with a slight change of notation, we denote $\mathcal{Q}_{M_1}$ for system 1 by $\{Q_1, Q_2, \ldots, Q_{D_1}\}$ and for system 2 with a prime by $\{Q'_1, Q'_2, \ldots, Q'_{D_1}\}$. Apart from these individual questions, $\mathcal{Q}_{M_2}$ should contain composite questions $Q_i * Q'_j$ for some connective $*$. Pairwise independence of $\mathcal{Q}_{M_2}$ enforces that $*$ must satisfy the following truth table, where 'yes'$= 1$ and 'no'$= 0$ (Q_i, Q'_j are compatible) [1]:

Q_i	Q'_j	$Q_i * Q'_j$
0	1	a
1	0	a
1	1	b
0	0	b

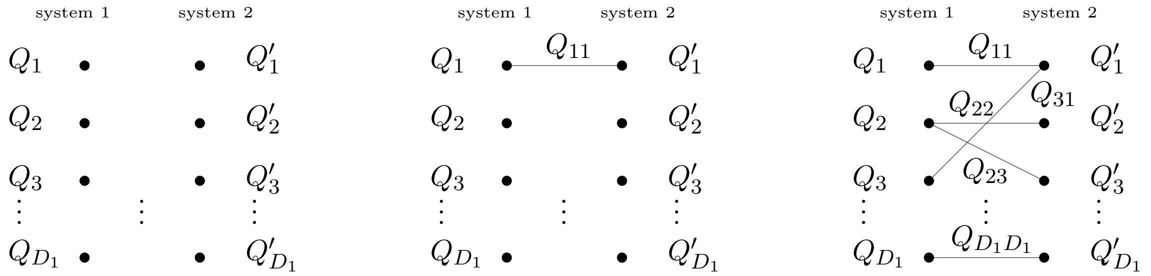
$$a \neq b \qquad a, b \in \{0, 1\}. \tag{5}$$

Hence, $*$ is either the XNOR $\leftrightarrow$ (for $a = 0$, $b = 1$), or its negation, the XOR $\oplus$ (for $a = 1$, $b = 0$). Up to an overall negation $\neg$, the two connectives are logically equivalent and so we henceforth make the convention to only build up composite questions (for informationally complete sets) using the XNOR. The composite question $Q_{ij} = Q_i \leftrightarrow Q'_j$ is a 'correlation question', representing "are the answers to Q_i, Q'_j the same?." Ultimately, in quantum theory, $\leftrightarrow$ will turn out to correspond to the tensor product $\otimes$ in $\sigma_i \otimes \sigma_j$ where σ_i is a Pauli matrix; Q_{ij} will then correspond to "are the spins of qubit 1 in i- and of qubit 2 in j-direction correlated?."

[5] A Hermitian operator on $\mathbb{C}^{2^N}$ is a Pauli operator iff it has two eigenvalues ± 1 of equal multiplicity.

4.2. Question graphs, independence and compatibility for $N = 2$ and entanglement

It is convenient to represent questions graphically: individual questions are represented as *vertices* and bipartite correlation questions as *edges* between them. For instance, we may have



Since O is only allowed to connect compatible questions logically, there can be no edge between individual questions of the *same* system.

Using only principles 1 and 2 and logical arguments, the following result is proven in [1]:

Lemma 1. *Q_i, Q'_j, Q_{ij} are pairwise independent for all $i, j = 1, \ldots, D_1$ and will thus be part of an informationally complete set $\mathcal{Q}_{M_2}$. Furthermore:*

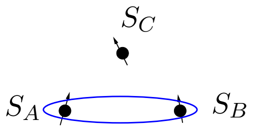
(i) Q_i is compatible with Q_{ij}, $\forall\, j = 1, \ldots, D_1$ and complementary to Q_{kj}, $\forall\, k \neq i$ and $\forall\, j = 1, \ldots, D_1$. That is, graphically, an individual question Q_i is compatible with a correlation question Q_{ij} if and only if its corresponding vertex is a vertex of the edge corresponding to Q_{ij}. By symmetry, the analogous result holds for Q'_j.

(ii) Q_{ij} and Q_{kl} are compatible if and only if $i \neq k$ and $j \neq l$. That is, graphically, Q_{ij} and Q_{kl} are compatible if their corresponding edges do not *intersect in a vertex and complementary if they intersect in one vertex.*

For example, Q_1 in the third question graph above is compatible with Q_{11} and complementary to Q_{22}, while Q_{11} and Q_{22} are compatible and Q_{11} and Q_{31} are complementary.

This lemma has a striking consequence: it implies *entanglement*. Indeed, since, e.g., Q_{11} and Q_{22} are independent and compatible, O may spend his maximally accessible amount of $N = 2$ *independent* `bits` of information (principle 1) over correlation questions only. Since nonintersecting edges do not share a common vertex, the lemma implies that no individual question is simultaneously compatible with two correlation questions that are compatible. Hence, when knowing the answers to Q_{11}, Q_{22}, O will be entirely ignorant about the individual questions; O has then maximal information about S_2, but purely composite information. This is entanglement in the very sense of Schrödinger (*"...the best possible knowledge of a whole does not necessarily include the best possible knowledge of all its parts..."* [16]). For example, in quantum theory, a state with $Q_{11} = Q_{22} =$ 'yes' will coincide with a Bell state having the spins of qubits 1 and 2 correlated in x- and y-direction (and anti-correlated in z-direction). Of course, there is nothing special about Q_{11}, Q_{22} and the argument works similarly for other composite question pairs and can be extended also to states with non-maximal entanglement (see [1] for details).

For systems with limited information content, *entanglement is therefore a direct consequence of complementarity*; without it there would be no independent and compatible composite questions sufficient to saturate the information limit [1]. For instance, two classical bits satisfy principle 1 as well, but admit no complementarity so that $\mathcal{Q}^{\rm cbit}_{M_2} = \{Q_1, Q'_1, Q_{11}\}$ and the maximum amount of $N = 2$ *independent* bits can*not* be spent on composite questions only.



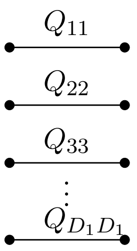
We also note that principles 1 and 2 offer a simple, intuitive explanation for *monogamy of entanglement*. Consider, for a moment $N = 3$ elementary systems S_A, S_B, S_C, and suppose S_A and S_B are maximally entangled (say, because O received the answer $Q_{11} = Q_{22} =$ 'yes' from S_{AB}). Noting that S_{AB} is a composite bipartite system inside the tripartite S_{ABC}, O has then already spent his maximal amount of information of $N = 2$ *independent* `bits` which he may know about S_{AB} and can therefore not know anything else that is independent, incl. non-trivial correlations with S_C, about the pair. To saturate the $N = 3$ *independent* bit limit for the tripartite system S_{ABC}, he may then only inquire individual information about S_C. This is *monogamy* in its extreme form: the maximally entangled pair S_{AB} can*not* be entangled with any other system S_C. This heuristic argument can be made rigorous in terms of the compatibility and independence structure of questions for $N \geq 3$ and can be extended to the non-extremal case using informational *monogamy inequalities* [1].

4.3. A logical explanation for the three-dimensionality of the Bloch ball

A key result of the reconstruction, proven in [1], is the following. Since its proof is instructive and representative for this approach, we shall rephrase it here.

Theorem 1. $D_1 = 2$ *or* 3.

Proof. Consider the $N = 2$ case. Lemma 1 implies that any maximal set of pairwise compatible correlation questions has D_1 elements. Indeed, there are maximally D_1 non-intersecting edges between the D_1 vertices of system 1 and the D_1 vertices of system 2; e.g., the D_1 'diagonal' Q_{ii}



are pairwise independent and compatible. The constraints on the posterior state update rule in section 2.4 entail that they are also mutually compatible (Specker's principle) [1] such that O may simultaneously know the answers to all D_1 Q_{ii}. Since O may not know more than $N = 2$ independent `bits` (principle 1), the D_1 Q_{ii} can*not* be mutually independent. Thus, assuming the Q_{ii} are of equivalent status, the answers to any pair of them, say Q_{11}, Q_{22}, must imply the answers to all others, say Q_{ii}, $i = 3, \ldots, D_1$. Hence, $Q_{jj} = Q_{11} * Q_{22}$, $j \neq 1, 2$, for a connective $*$ that preserves pairwise independence of Q_{11}, Q_{22}, Q_{jj}. Reasoning as in (5) implies that either

$$Q_{jj} = Q_{11} \leftrightarrow Q_{22}, \qquad \text{or} \qquad Q_{jj} = \neg(Q_{11} \leftrightarrow Q_{22}), \qquad j = 3, \ldots, D_1 \tag{6}$$

so that for $D_1 > 3$ Q_{jj}, $j = 3, \ldots, D_1$, can*not* be pairwise independent. Arguing identically for all other sets of D_1 pairwise independent and compatible Q_{ij}, we conclude that $D_1 \leq 3$. □

This theorem has several crucial repercussions. We may already suggestively call $D_1 = 2$ and $D_1 = 3$ the 'rebit' (two-level systems over *real* Hilbert spaces) and 'qubit' case, respectively. Reasoning as in (6) shows that the Q_{ij} are logically closed under $\leftrightarrow$; as demonstrated in [1]:

Theorem 2. *If* $D_1 = 3$ *then* $\mathcal{Q}_{M_2} := \{Q_i, Q'_j, Q_{ij}\}_{i,j=1,2,3}$ *is logically closed under* $\leftrightarrow$ *and thus constitutes an informationally complete set for* $N = 2$ *with* $D_2 = 15$.

If $D_1 = 2$ *then* $\mathcal{Q}_{M_2} = \{Q_i, Q'_j, Q_{ij}, Q_{11} \leftrightarrow Q_{22}\}_{i,j=1,2}$ *is logically closed under* $\leftrightarrow$ *and thus constitutes an informationally complete set for* $N = 2$ *with* $D_2 = 9$*. Furthermore,* $Q_{11} \leftrightarrow Q_{22}$ *is complementary to the individual questions* Q_i, Q'_j*,* $i, j = 1, 2$.

Indeed, $D_2 = 9, 15$ are the correct numbers of degrees of freedom for $N = 2$ rebits and qubits, respectively. However, since the composite question $Q_{11} \leftrightarrow Q_{22}$ is complementary to *all* individual questions in the rebit case (this is *not* true in the qubit case!), it is impossible for O to do ensemble state tomography by asking only individual questions Q_i, Q'_j, thereby violating principle 6. We are left with the qubit case and shall henceforth ignore rebits (for rebits see [1]).

4.4. The correlation structure for $N = 2$ and ruling out local hidden variables

Using (6) and repeating the argument leading to it for 'non-diagonal' Q_{ij} shows that either

$$Q_{11} \leftrightarrow Q_{22} = Q_{12} \leftrightarrow Q_{21}, \qquad \text{or} \qquad Q_{11} \leftrightarrow Q_{22} = \neg(Q_{12} \leftrightarrow Q_{21}). \tag{7}$$

The first case (without relative negation) is the case of *classical* logic and compatible with *local* hidden variables for the individual questions Q_i, Q'_j. Namely, note that $Q_{11} \leftrightarrow Q_{22} = Q_{12} \leftrightarrow Q_{21}$ can be rewritten in terms of the individuals as

$$(Q_1 \leftrightarrow Q'_1) \leftrightarrow (Q_2 \leftrightarrow Q'_2) = (Q_1 \leftrightarrow Q'_2) \leftrightarrow (Q_2 \leftrightarrow Q'_1). \tag{8}$$

Suppose for a moment that Q_1, Q'_1, Q_2, Q'_2 had simultaneous definite values (although not accessible to O). It is easy to convince oneself that any distribution of simultaneous truth values over the Q_i, Q'_j satisfies (8) [1]. In fact, (8) is a *classical logical identity* and can be argued to follow from classical rules of inference [1]. However, it involves complementary individual questions, thereby violating our premise from section 2.7 that O may apply classical rules of inference exclusively to mutually compatible questions. This classical case is thus ruled out.

One can check that the second case, $Q_{11} \leftrightarrow Q_{22} = \neg(Q_{12} \leftrightarrow Q_{21})$, does *not* admit a *local* hidden variable interpretation, but is consistent with the structure of the theory landscape and principles [1]. Since one of the two cases (7) *must* be true, we conclude that this second case holds. In fact, for *any* complementary pairs Q, Q' and Q'', Q''' such that both Q and Q' are compatible with both Q'', Q''', one finds similarly [1]

$$(Q \leftrightarrow Q'') \leftrightarrow (Q' \leftrightarrow Q''') = \neg\left((Q \leftrightarrow Q''') \leftrightarrow (Q' \leftrightarrow Q'')\right). \tag{9}$$

This precludes to reason classically about the distribution of truth values over O's questions.

(9) permits us to unravel the complete correlation structure for $\mathcal{Q}_{M_2}$. In fact, it turns out that there are two distinct representations of this correlation structure: one corresponding to quantum theory in its standard representation, the other to its 'mirror' representation, related by a *passive* (not a physical) transformation, reassigning $Q_1 \mapsto \neg Q_1$ (in quantum theory tantamount to a partial transpose on qubit 1) [1]. The two distinct representations turn out to be physically equivalent and so a convention has to be made. Choosing the 'standard' case and using (9), one finds that the compatibility and correlation structure of $\mathcal{Q}_{M_2}$ can be represented graphically as in fig. 1. For Q, Q', Q'' compatible, we shall henceforth distinguish between

even correlation: if $Q = Q' \leftrightarrow Q''$, and

odd correlation: if $Q = \neg(Q' \leftrightarrow Q'')$.

One can easily check that quantum theory satisfies this correlation structure for projective spin measurements if one replaces $i = 1, 2, 3$ by x, y, z. For instance, $Q_{11} = Q_{22} =$ 'yes' implies, by fig. 1, the dependent $Q_{33} =$ 'no'. In quantum theory, this corresponds to the (unnormalized) Bell state with spin correlation in x- and y-direction and anti-correlated spins in z-direction

$$|x_+x_+\rangle - |x_-x_-\rangle = -i|y_+y_+\rangle + i|y_-y_-\rangle = |z_+z_-\rangle + |z_-z_+\rangle.$$

4.5. Compatibility, independence and informational completeness for arbitrary N

Consider N elementary systems in the 'qubit' ($D_1 = 3$) case and the XNOR conjunction

$$Q_{\mu_1\mu_2\cdots\mu_N} := Q_{\mu_1} \leftrightarrow Q_{\mu_2} \leftrightarrow \cdots \leftrightarrow Q_{\mu_N} \tag{10}$$

of individual questions, where $\mu_a = 0, 1, 2, 3$ and $Q_0 := 1$. The conjunction yields 'yes' and 'no' if an even and odd number of $Q_{\mu_a} =$ 'no', respectively, and thus does *not* represent "are the answers to all Q_{μ_a} the same?." As shown in [1], these conjunctions are informationally complete:

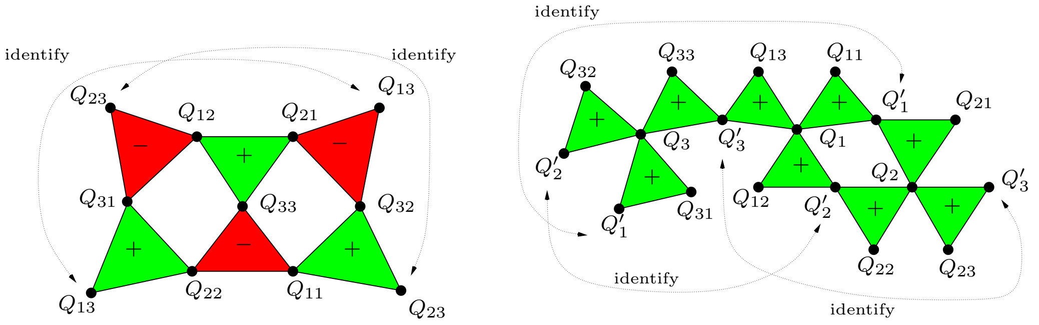


Figure 1. The compatibility and correlation structure of the informationally complete set $\mathcal{Q}_{M_2}$ for the $N = 2$ qubit case. Two questions are compatible if connected by a triangle edge and complementary otherwise. Red and green triangles denote odd and even correlation, respectively; e.g., $Q_{33} = \neg(Q_{11} \leftrightarrow Q_{22}) = Q_{12} \leftrightarrow Q_{21}$. (Taken from [1].)

Theorem 3. (Qubits) *The* $4^N - 1$ *questions*[6] $Q_{\mu_1 \cdots \mu_N}$, $\mu = 0, 1, 2, 3$, *are pairwise independent and logically closed under* $\leftrightarrow$ *and thus form an informationally complete set* $\mathcal{Q}_{M_N}$ *with* $D_N = 4^N - 1$. *Moreover,* $Q_{\mu_1 \cdots \mu_N}$ *and* $Q_{\nu_1 \cdots \nu_N}$ *are compatible if they differ by an* **even** *number (incl.* 0*) of non-zero indices and complementary otherwise.*

We note that an N-qubit density matrix has precisely $4^N - 1$ degrees of freedom.

4.6. Linear, reversible time evolution and a quadratic information measure

Thus far, the summarized results invoked only principles 1 and 2 (and in one instance principle 6). Principles 3 and 4, on the other hand, can be demonstrated to entail a *linear* and *reversible* evolution of the generalized Bloch vector $\mathbb{R}^{4^N - 1} \ni \vec{r} = 2\,\vec{y} - \vec{1}$ that already appeared in (4),

$$\vec{r}(\Delta t + t_0) = T(\Delta t)\,\vec{r}(t_0), \tag{11}$$

where $T(\Delta) \subset \mathcal{T}_N$ defines a one-parameter matrix group [1]. Suppose $T(\Delta t), T'(\Delta t') \in \mathcal{T}_N$ correspond to two distinct interactions to which O may subject S_N. By principle 4, $T(\Delta t) \cdot T'(\Delta t')$ must likewise be contained in $\mathcal{T}_N$ and since both T, T' are invertible, also the entire set $\mathcal{T}_N$ must be a group. We shall henceforth often represent states with Bloch vectors $\vec{r}$.

Principles 3 and 4, together with elementary operational conditions on the information measure, enforce it to be quadratic $\alpha(y_i) = (2\,y_i - 1)^2$ so that O's total information (1)

$$I_N(\vec{y}) = \sum_{i=1}^{4^N - 1} (2\,y_i - 1)^2 = |\vec{r}|^2 \tag{12}$$

is simply the square norm of the Bloch vector [1]. Interestingly, this derivation would not work without the *continuity* of time evolution (principle 4). Crucially, (12) is *not* the Shannon entropy (see [1] for a discussion why the Shannon entropy is also conceptually not suitable for quantifying O's information). This reconstruction thereby corroborates an earlier proposal for a quadratic information measure for quantum theory by Brukner and Zeilinger [13–15].

This quadratic information measure becomes key for the remaining steps of the reconstruction. Given that (12) is a 'conserved charge' of time evolution (principle 3), we can already infer that $\mathcal{T}_N \subset \mathrm{SO}(4^{\mathrm{N}} - 1)$ because time evolution must be connected to the identiy.

[6] We deduct the trivial question $Q_{000 \cdots 000}$.

4.7. Pure and mixed states

Suppose O knows S_N's answers to N mutually compatible questions from $\mathcal{Q}_{M_N}$, thereby saturating the information limit of N *independent* `bits` (principle 1). He will then also know the answers to each of their bipartite, tripartite, ..., and N-partite XNOR conjunctions which, by theorem 3, are also in $\mathcal{Q}_{M_N}$ (and compatible). In total, he then knows the answer to

$$\binom{N}{1}+\binom{N}{2}+\cdots\binom{N}{N}=\sum_{i=1}^{N}\binom{N}{i}=2^N-1$$

questions from $\mathcal{Q}_{M_N}$. Thus, O's total information (12) is 2^N-1 `bits` in this case. It contains *dependent* `bits` of information because the questions in $\mathcal{Q}_{M_N}$ are pairwise, but not all mutually independent. Thanks to principle 3, this is invariant under time evolution.

This allows us to distinguish two kinds of states [1]; $\vec{y}$ is called a

pure state: if it is a state of maximal information, and hence of maximal length

$$I_N(\vec{y})=\sum_{i=1}^{4^N-1}(2\,y_i-1)^2=(2^N-1)\,\texttt{bits}, \tag{13}$$

mixed state: if it is a state of non-maximal information,

$$0\,\texttt{bit}\leq I_N(\vec{y})=\sum_{i=1}^{4^N-1}(2\,y_i-1)^2<(2^N-1)\,\texttt{bits}. \tag{14}$$

The square length of the Bloch vector thus corresponds to the number of answered questions. The state of no information $\vec{y}=\frac{1}{2}\,\vec{1}$ has length 0 `bits`.

As can be easily checked, quantum theory satisfies this characterization. In particular, an N-qubit density matrix, corresponding to a pure state, has a Bloch vector with square norm equal to 2^N-1. This peculiar fact now has a clear informational interpretation.

4.8. The Bloch ball and unitary group for a qubit from a conserved informational charge

Since $D_1=3$ (cf. sec. 4.3), we have that $\mathcal{Q}_{M_1}=\{Q_1,Q_2,Q_3\}$ is a maximal set of mutually complementary questions, i.e., no further $Q\in\mathcal{Q}_1$ can be added to $\mathcal{Q}_{M_1}$ without destroying mutual complementarity in the set (cf. sec. 4.1). According to (13), a pure state satisfies

$$I_{N=1}(\vec{y})=r_1^2+r_2^2+r_3^2=(2\,y_1-1)^2+(2\,y_2-1)^2+(2\,y_3)^2=1\,\texttt{bit}. \tag{15}$$

For later, we thus observe: *for pure states, the maximal mutually complementary set carries* exactly 1 ***bit*** *of information and this is a conserved charge of time evolution (principle 3).*

Principle 1 implies that, e.g., the pure state $\vec{y}_*=(1,0,0)$ exists in Σ_1 and we know $\mathcal{T}_1\subset\mathrm{SO}(3)$. But it is clear that applying *any* $T\in\mathrm{SO}(3)$ to $\vec{y}_*$, according to (11), yields only states that are also compatible with all principles 1–3 (and the landscape). Hence, by principle 4 we must actually have $\mathcal{T}_1=\mathrm{SO}(3)\simeq\mathrm{PSU}(2)$. Clearly, $\mathcal{T}_1$ then generates *all* quantum pure states from $\vec{y}_*$, i.e., it yields the entire Bloch sphere (the image of any legal state under a legal time evolution is also a legal state). Recalling that Σ_1 is convex, we obtain that $\Sigma_1=B^3\simeq$ convex hull of $\mathbb{CP}^1$ is the entire unit Bloch ball with mixed states (14) lying inside; the completely mixed state equals the state of no information at the center. $\Sigma_1,\mathcal{T}_1$ coincide exactly with the set of density matrices $\rho=\frac{1}{2}(\mathbb{1}+\vec{r}\cdot\vec{\sigma})$ and the set of unitary transformations $\rho\mapsto U\,\rho\,U^\dagger$, $U\in\mathrm{SU}(2)$, respectively, for a single qubit in its *adjoint* (i.e., Bloch vector) representation, where $\vec{\sigma}=(\sigma_1,\sigma_2,\sigma_3)$ is the vector of Pauli matrices. Finally, from the assumptions in sec. 2.8 and principle 5 it is also clear that

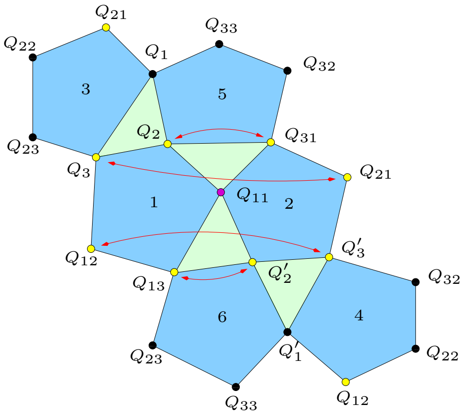


Figure 2. The six maximal complementarity sets represented as pentagons. Two questions are complementary if they share a pentagon or are connected by an edge and compatible otherwise. Every pentagon is connected to all other five because any $Q \in \mathcal{Q}_{M_2}$ is contained in precisely two pentagons. The red arrows represent the information swap (21) between pentagons 1 and 2 that preserves all pentagon equalities (18) and defines the time evolution generator (22). (Figure adapted from [2].)

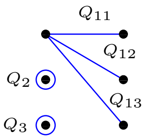
$\mathcal{Q}_1 = \{\vec{q} \in \mathbb{R}^3 \,|\, |\vec{q}|^2 = 1\,\texttt{bit}\} \simeq \mathbb{CP}^1$. This coincides with the set of projectors $P_{\vec{q}} = \frac{1}{2}(\mathbb{1} + \vec{q}\cdot\vec{\sigma})$ onto the $+1$ eigenspaces of the Pauli operators $\vec{q}\cdot\vec{\sigma}$. Noting that

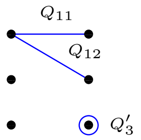
$$\mathrm{Tr}(\rho\, P_{\vec{q}}) = \frac{1}{2}(1 + \vec{r}\cdot\vec{q}) \equiv Y(Q|\vec{y}) \tag{16}$$

we also recover that (4) yields the Born rule for projective measurements. We thus have the claim of sec. 3 for $N = 1$ (for details see [1, 2]).

4.9. Unitary group and density matrices for two qubits from conserved informational charges

Also for $N = 2$ it is rewarding to consider maximal mutually complementary sets within $\mathcal{Q}_{M_2}$. Using lemma 1, one can check that there are exactly *six* maximal complementarity sets containing five questions and *twenty* containing three [2]; e.g., two graphical representatives are:





$$\mathrm{Pent}_1 = \{Q_{11}, Q_{12}, Q_{13}, Q_2, Q_3\}, \qquad \mathrm{Tri}_1 = \{Q_{11}, Q_{12}, Q_3'\}\,.$$

The six maximal complementarity sets of five elements can be represented as a lattice of pentagon, see fig. 2 (which also contains four green triangles, each representing one of the twenty maximal complementarity sets of three questions) [2].

Each of these sets has to satisfy the complementarity inequalities (2); specifically $0\,\texttt{bits} \le I(\mathrm{Pent}_a) := \sum_{i\in\mathrm{Pent}_a} r_i^2 \le 1\,\texttt{bit}$ for the information carried by the five questions in pentagon a. Since any $Q \in \mathcal{Q}_{M_2}$ is contained in precisely two pentagons (cf. fig. 2) we find

$$\sum_{a=1}^{6} I(\mathrm{Pent}_a) = 2\left(\sum_{i=1,2,3}(r_{i_1}^2 + r_{i_2}^2) + \sum_{i,j=1,2,3} r_{ij}^2\right) = 2\,I_{N=2}(\vec{r}). \tag{17}$$

Noting that for pure states $I_{N=2}(\vec{r}_{\mathrm{pure}}) = 3\,\texttt{bits}$ thus produces the *pentagon equalities* [2]

$$\textbf{pure states:} \qquad I(\mathrm{Pent}_a) \equiv 1\,\texttt{bit}, \qquad a = 1, \ldots, 6. \tag{18}$$

Any pure state *must* satisfy (18) and $\mathcal{T}_2$ evolves pure states to pure states (principle 3). Hence, in analogy to $N = 1$: *for pure states, these six maximal mutually complementary sets carry* exactly 1 ***bit*** *of information and these are six conserved charges of time evolution.* There are further interesting constraints on the distribution of O's information over $\mathcal{Q}_{M_2}$ [2].

It can be straightforwardly checked that quantum theory actually satisfies (18). Indeed, in the case of quantum theory the identity for Pent_1 reads in more familiar language (pure states)

$$I(\text{Pent}_1) = \langle\sigma_2 \otimes \mathbb{1}\rangle^2 + \langle\sigma_3 \otimes \mathbb{1}\rangle^2 + \langle\sigma_1 \otimes \sigma_1\rangle^2 + \langle\sigma_1 \otimes \sigma_2\rangle^2 + \langle\sigma_1 \otimes \sigma_3\rangle^2 = 1,$$

etc. Remarkably, these identities of quantum theory seem not to have been reported before in the literature. These novel conserved informational charges are a prediction of our reconstruction, underscoring the benefits of taking this informational approach. They will become indispensable.

Using that $I(\text{Pent}_a(\vec{r}))$ is conserved under $\mathcal{T}_2 \subset \text{SO}(15)$ entails (with new index $i = 1, \dots, 15$)

$$\sum_{i\in\text{Pent}_a, 1\leq j\leq 15} r_i\, G_{ij}\, r_j = 0, \qquad\qquad a = 1, \dots 6, \tag{19}$$

where $T(\Delta t) = \exp(\Delta t G)$ for $G \in \mathfrak{so}(15)$ [2]. The correlation structure of fig. 1 enforces [2]

$$G_{ij} = 0, \qquad\qquad \text{whenever } Q_i, Q_j \text{ are compatible.} \tag{20}$$

Each of the 15 $Q_i \in \mathcal{Q}_{M_2}$ is complementary to eight others and since $G_{ij} = -G_{ji}$, there could be maximally 60 linearly independent G_{ij} of $\mathcal{T}_2$.

These are constructed as follows. For *every* pair of pentagons there is a unique information swap transformation which preserves (18). For instance, the red arrows in fig. 2 represent the complete information swap between pentagons Pent_1 and Pent_2 ($\longleftrightarrow$ is *not* the XNOR)

$$r_2^2 \longleftrightarrow r_{31}^2\ (\text{Pent}_5),\ r_3^2 \longleftrightarrow r_{21}^2\ (\text{Pent}_3),\ r_{12}^2 \longleftrightarrow {r'_3}^2\ (\text{Pent}_4),\ r_{13}^2 \longleftrightarrow {r'_2}^2\ (\text{Pent}_6) \tag{21}$$

that keeps all other components fixed. (18) are preserved because every swap in (21) occurs within a pentagon. The correlation structure of fig. 1 fixes the corresponding generator to [2]

$$G_{ij}^{\text{Pent}_1,\text{Pent}_2} = \delta_{i1}\delta_{j(31)} - \delta_{i3}\delta_{j(21)} + \delta_{i(12)}\delta_{j3'} - \delta_{i(13)}\delta_{j2'} - (i \longleftrightarrow j). \tag{22}$$

One can repeat the argument for all 15 pentagon pairs, producing 15 linearly independent generators [2]. Remarkably, they turn out to coincide exactly with the adjoint representation of the 15 fundamental generators of SU(4) [2]. In particular, (22) is the generator of entangling unitaries leaving r_{11} invariant. The other 45 independent generators satisfying (20) are ruled out by the correlation structure so that $\mathcal{T}_2$ cannot be generated by anything else than these 15 pentagon swaps [2]. One can show that the exponentiation of (linear combinations of) these 15 pentagon swaps generates PSU(4) and that this group abides by all principles and forms a maximal subgroup of SO(15) [2]. Principle 4 then implies $\mathcal{T}_2 \simeq \text{PSU}(4)$ which is the correct set of unitary transformations $\rho \mapsto U\,\rho\,U^\dagger$, $U \in \text{SU}(4)$, for two qubits.

It turns out that the set of Bloch vectors satisfying all six pentagon equalities (18) and the conservation equations (19) for the 15 pentagon swaps splits into two sets on each of which $\mathcal{T}_2 = \text{PSU}(4)$ acts transitively [2]. These two sets correspond precisely to the two possible conventions of building up composite questions either using the XNOR or XOR (cf. sec. 4.1) and are therefore physically equivalent. Adhering to the XNOR convention, we conclude that the surviving set of Bloch vectors solving (18, 19) is the set of $N = 2$ states admitted by the principles. Indeed, it coincides exactly with the set of quantum pure states which forms a $\mathbb{CP}^3$ of which PSU(4) is the isometry group [2]. Employing convexity of Σ_2, one finally finds

$$\Sigma_2 = \text{closed convex hull of } \mathbb{CP}^3,$$

which is exactly the set of normalized 4×4 density matrices over $\mathbb{C}^2 \otimes \mathbb{C}^2$.

Concluding, the new conserved informational charges (18), in analogy to (15) for $N = 1$, define both the unitary group and set of states for two qubits. (For neglected details, see [2].)

4.10. Unitaries and states for $N > 2$ elementary systems

According to theorem 3, Σ_N is $(4^N - 1)$-dimensional and $\mathcal{T}_N \subset \mathrm{SO}(4^{\mathrm{N}} - 1)$ (cf. sec. 4.6). The reconstruction of the unitary group uses a *universality* result from quantum computation: two-qubit unitaries PSU(4) (between any pair) and single-qubit unitaries $\mathrm{PSU}(2) \simeq \mathrm{SO}(3)$ generate the full projective unitary group $\mathrm{PSU}(2^{\mathrm{N}})$ for N qubits [17, 18]. Given that S_N is a composite system, all of these bipartite and local unitaries must be in $\mathcal{T}_N$. One can check that $\mathrm{PSU}(2^{\mathrm{N}})$ again abides by all principles and constitutes a maximal subgroup of $\mathrm{SO}(4^{\mathrm{N}} - 1)$ [2]. Thanks to principle 4, this yields $\mathcal{T}_N \simeq \mathrm{PSU}(2^{\mathrm{N}})$ which coincides with the set of unitary transformation on N-qubit density matrices. In analogy to the previous case, one obtains as the state space

$$\Sigma_N = \text{closed convex hull of } \mathbb{CP}^{2^N-1},$$

which agrees with the set of normalized N-qubit density matrices. (For details, see [2].)

4.11. Questions as projective measurements and the Born rule

The assumptions in sec. 2.8 and principle 5 yield the following question set characterization [2]:

$$\mathcal{Q}_N \simeq \{\vec{q} \in \mathbb{R}^{4^N-1} \,|\, Y(\vec{q}|\vec{r}) \in [0,1] \,\forall\, \vec{r} \in \Sigma_N \quad \text{and} \quad \vec{q} \quad \text{is a 1 } \texttt{bit} \text{ quantum state}\}. \tag{23}$$

As shown in [2], this set is ismorphic to the set of projectors $P_{\vec{q}} = \frac{1}{2}(\mathbb{1} + \vec{q} \cdot \vec{\sigma})$ onto the $+1$ eigenspaces of the Pauli operators $\vec{q} \cdot \vec{\sigma} = \sum_{\mu_a \cdots \mu_N} q_{\mu_1 \cdots \mu_N} \sigma_{\mu_1 \cdots \mu_N}$, where $\sigma_{\mu_1 \cdots \mu_N} = \sigma_{\mu_1} \otimes \cdots \otimes \sigma_{\mu_N}$ and $\sigma_0 = \mathbb{1}$. Noting that $q_{\mu_1 \cdots \mu_N}$ corresponds to (10) reveals that the XNOR at the question level corresponds to the tensor product $\otimes$ at the operator level. One also finds that (16) again holds such that (4) yields the Born rule for projective measurements for arbitrary N. (For the neglected details and many further interesting properties of $\mathcal{Q}_N$, we refer to [2].)

4.12. The von Neumann evolution equation

We thus obtain qubit quantum theory in its adjoint (i.e. Bloch vector) representation. Lastly, we note that $\vec{r}(t) = T(t)\,\vec{r}(0)$ with $T(t) = e^{t\,G} \in \mathrm{PSU}(2^{\mathrm{N}})$ is equivalent to the adjoint action

$$\rho(t) = U(t)\,\rho(0)\,U^\dagger(t), \tag{24}$$

of $U(t) = e^{-i\,H\,t} \in \mathrm{SU}(2^N)$ for some hermitian operator H on $\mathbb{C}^{2^N}$, where $\rho(t) = \frac{1}{2^N}\left(\mathbb{1} + \vec{r}(t) \cdot \vec{\sigma}\right)$ [2]. (24), in turn, is equivalent to $\rho(t)$ solving the von Neumann evolution equation

$$i\frac{\partial\,\rho}{\partial t} = [H, \rho]. \tag{25}$$

We have therefore also recovered the correct time evolution equation for quantum states.

5. Conclusions

We have reviewed and summarized the key steps from [1, 2] necessary to prove the claim of sec. 3. This yields a reconstruction of the explicit formalism of qubit quantum theory from rules constraining an observer's acquisition of information about a system [1, 2]. The derivation corroborates the consistency of interpreting the state as the observer's 'catalogue of knowledge' and shows that it is sufficient to speak only about the information accessible to him for reproducing quantum theory. In fact, for qubits, this derivation accomplishes an informational reconstruction of the type proposed in Rovelli's *relational quantum mechanics* [11] and in the Brukner-Zeilinger informational interpretation of quantum theory [12, 13].

As a key benefit, this reconstruction also provides a novel informational explanation for the architecture of qubit quantum theory. In particular, it explains the logical structure of a basis of spin measurements, the dimensionality and structure of quantum state spaces, the correlation structure and the unitarity of time evolution from the perspective of information acquisition. This unravels previously unknown structural properties: conserved informational charges from complementarity relations define and explain the unitary group and the set of pure states.

Acknowledgments

The author thanks C. Wever for an enjoyable collaboration on [2]. The project leading to this publication has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie grant agreement No 657661.

References

[1] Höhn P 2014, *arXiv:1412.8323*

[2] Höhn P and Wever C 2015, *arXiv:1511.01130*, to appear in *Phys. Rev.* A

[3] Hardy L 2001, *arXiv:quant-ph/0101012*

[4] Dakic B and Brukner C 2011 in *Deep Beauty*, Ed Halvorson H (Cambridge University Press) pp. 365

[5] Masanes L and Müller M 2011, *New J. Phys.* **13**, 063001

[6] Chiribella G, D'Ariano G and Perinotti P 2011, *Phys. Rev. A* **84** 012311

[7] Barnum H, Müller M and Ududec C 2014, *New J. Phys.* **16** 123029

[8] de la Torre G, Masanes L, Short A and Müller M 2012, *Phys. Rev. Lett.* **109** 090403

[9] Goyal P 2010, *New J. Phys.* **12** 023012

[10] Appleby M, Fuchs C, Stacey B and Zhu H 2016, *arXiv:1612.03234*

[11] Rovelli R 1996, *Int. J. Theor. Phys.* **35** 1637

[12] Zeilinger A 1999, *Found. Phys.* **29** 631

[13] Brukner C and Zeilinger A 2003, in *Time, Quantum and Information*, Ed Castell L and Ischebeck O (Springer)

[14] Brukner C and Zeilinger A 1999, *Phys. Rev. Lett.* **83** 3354

[15] Brukner C and Zeilinger A 2001, *Phys. Rev. A* **63** 022113

[16] Schrödinger E 1935, *Math. Proc. Camb. Phil. Soc.* **31** 555

[17] Bremner M et al 2002, *Phys. Rev. Lett.* **89** 247902

[18] Harrow A 2009, *Quant. Inf. Comput.* **9** 773